Génération d'un certificat BNB

Comment

- *générer,*
- *renouveler (renewal) ou*
- *régénérer (recovery)*

un certificat de la Banque nationale de Belgique (BNB)?

Table des Matières

1. OBJECTIF DE CE MODE D'EMPLOI 3
2. INSTRUCTIONS DE SÉCURITÉ 3
3. CONDITIONS D'UTILISATION 3
4. PROCÉDURE DE GÉNÉRATION ET D'INSTALLATION D'UN CERTIFICAT BNB 4
5. PROCÉDURE DE RENOUVELLEMENT D'UN CERTIFICAT BNB (RENEWAL) 6
6. PROCÉDURE DE RÉGÉNÉRATION D'UN CERTIFICAT BNB (RECOVERY) 8
7. PROCÉDURE D'EXPORT, DE SAUVEGARDE/RESTAURATION ET DE SUPPRESSION DE CLÉS ET CERTIFICATS BNB 10
8. PROCÉDURE DE DÉCHARGEMENT DU PROGRAMME FACULTATIF « OFFLINE SIGNING TOOLS » (OST) .. 11
9. PROCÉDURES SPÉCIALES 12

Gestion des Versions

Datum	Beschrijving	Auteur
2007-09-24	Version de base	Luc CERTYN
2015-01-20	Adaptation URL	Rogier VANHERPE

1. OBJECTIF DE CE MODE D'EMPLOI

Ce mode d'emploi décrit les étapes qu'un correspondant externe de la BNB doit suivre pour générer, renouveler (« renewal »), régénérer (« recovery ») ou sauvegarder un certificat de la Banque nationale de Belgique.

D'autre part, on trouvera aussi les instructions pour décharger et utiliser le programme facultatif « Offline Signing Tool » (OST).

2. INSTRUCTIONS DE SÉCURITÉ

Le Password initial et l'Activation code reçus de la BNB (sous enveloppe fermée) doivent être CONSERVÉS en lieu SÛR.

Dans la « Procédure de génération et d'installation d'un certificat », il est prescrit de changer le Password initial. Veuillez également CONSERVER ce NOUVEAU Password en lieu SÛR.

3. CONDITIONS D'UTILISATION

- Le correspondant externe doit avoir remis une demande de certificat auprès de la BNB afin de l'employer dans une application BNB.

- Le correspondant externe marque son accord avec les documents : « Banque Nationale de Belgique - Certificate Policy » et « Banque Nationale de Belgique - Certificate Practice Statement For External CounterParties ».

- Le correspondant externe doit s'être présenté personnellement auprès d'une Autorité d'Enregistrement de la BNB.

- Le correspondant externe dispose d'un **Username** (parfois aussi appelé **NUIN** pour NBB Unique Identification Number), d'un **Password** pour se connecter et d'un Activation Code pour la génération du certificat. Ces données sont remises PERSONNELLEMENT par l'Autorité d'Enregistrement de la BNB au correspondant externe.

- Le correspondant externe dispose d'un PC avec Windows 2000SP2 ou Windows XPSP2 avec Internet Explorer version 6 ou 7.

Note: La clé privée et le certificat générés dans le browser Internet Explorer via cette application sont uniquement protégés par l'authentification Windows (il n'y a ni alerte ni mot de passe spécifique à fournir au moment de l'utilisation de la clé privée ; l'activation d'un de ces mécanismes de sécurité est toutefois possible via l'option « Enable strong private key protection. », comme indiqué dans la note du chapitre 3 « Comment restaurer une clé privée et son certificat » du document « Gestion des certificats en Internet Explorer »). Le correspondant externe responsable doit veiller à ce que le ou les comptes utilisateurs Windows qui donnent accès à ces informations soient correctement sécurisés (par exemple: mot de passe complexe, blocage du compte en l'absence de l'utilisateur, ...) et accessibles seulement aux personnes qui en ont besoin.

4. PROCÉDURE DE GÉNÉRATION ET D'INSTALLATION D'UN CERTIFICAT BNB

1. Dans le Browser Internet, spécifiez l'URL (parfois aussi appelée adresse Internet):
   https://ssl.nbb.be/nbbxenroll

2. Vous recevez un écran invitant à introduire un **Username** et **Password**.

3. Introduisez les **Username** et **Password** (reçus de la BNB) et cliquez sur Log In

4. A la première connexion, vous êtes invités à modifier immédiatement le Password initial que vous avez reçu de la BNB. Le Password que vous choisirez doit posséder au moins 8 caractères (avec un maximum de 16) et comprendre au moins une minuscule, une majuscule et un chiffre. Procédez comme suit:
   - Tapez le Password reçu dans le champ **Old password**.
   - Tapez un nouveau Password dans le champ **New password**.
   - Tapez encore une fois ce nouveau Password dans le champ **Confirm password**.
   - Cliquez sur Apply pour effectuer le changement de mot de passe. Note: le bouton Reset efface le contenu de tous les champs.
   - Après avoir reçu le message confirmant le changement de Password, cliquez sur Continue.

5. Installer le **Root CA** Certificate. Procédez comme suit :
   - Cliquez sur **Downloads**
   - Cliquez sur **Root CA certificate**
   - Dans la boîte de dialogue, cliquez sur Open
   - Le certificat apparaît dans une nouvelle fenêtre ; dans cette fenêtre, cliquez sur Install Certificate...
   - Dans le Wizard d'importation de certificat, cliquez sur Next >
   - Assurez-vous que l'option « Automatically select the certificate store based on the type of certificate » est sélectionnée et cliquez sur Next >
   - Dans l'écran suivant, cliquez sur Finish
   - Si vous recevez un message de « Security Warning » pour l'installation d'un certificat de « certification authority (CA) », cliquez sur Yes.
     - *Note: le « Thumbprint (sha1) » de la « National Bank of Belgium – ROOT CA » est 184AA4F8 32D2CC4B 9E0AA534 461054D2 1C4EB5C6.*
   - Lorsque vous recevez le message « The import was successful. », cliquez sur OK
   - Cliquez sur OK dans la fenêtre « Certificate » restée ouverte pour la refermer.

6. Installer le **CA** Certificate. Procédez comme suit :
   - Cliquez sur **CA certificate**
   - Dans la boîte de dialogue, cliquez sur Open
   - Génération d'un certificat BNB
   - Le certificat apparaît dans une nouvelle fenêtre ; cliquez sur Install Certificate...
   - Dans le Wizard d'importation de certificat, cliquez sur Next >
   - Assurez-vous que l'option « Automatically select the certificate store based on the type of certificate » est sélectionnée et cliquez Next >
   - Dans l'écran suivant, cliquez sur Finish
   - Lorsque vous recevez le message « The import was successful. », cliquez sur OK
   - Cliquez sur OK dans la fenêtre « Certificate » restée ouverte pour la refermer.

7. Cliquez sur **Certificate Request**

8. Avant de générer un certificat, vous devez lire et accepter les conditions des « NBB Certificate Policy » et « NBB Certificate Practice Statement ». Les dernières versions de ces documents sont consultables via les liens repris à gauche de la page.

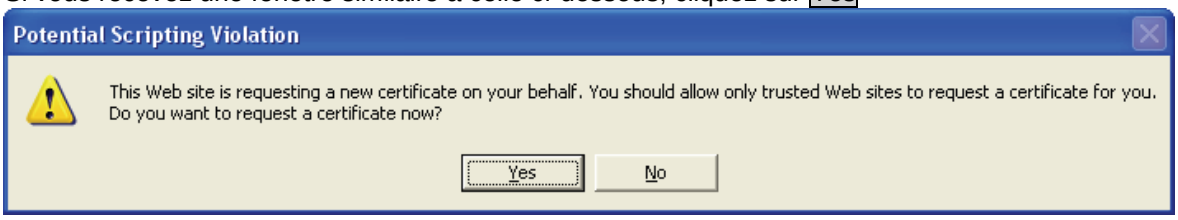
9. Pour marquer votre accord sur ces documents, vous devez cocher la case **I have read and accept the latest Certificate Policy and Certificate Practice Statement documents**. C'est seulement après cette action que le bouton Request certificate deviendra actif.

10. Le champ Email contient l'adresse e-mail qui sera reprise dans le certificat. Cette information est obligatoire et peut être utilisée par la banque pour vous contacter. Si l'adresse indiquée n'est pas correcte, veuillez la modifier.

11. Complétez le champ **Activation code** avec le code que vous avez reçu de la Banque.

12. Cliquez sur le bouton Request certificate.

13. Si vous recevez une fenêtre similaire à celle ci-dessous, cliquez sur Yes


Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
Yes
No

14. Votre PC va générer une clé cryptographique et demander à l'AC BNB de créer le certificat associé. Après quelques instants, vous allez recevoir un écran vous invitant à charger ce certificat dans votre browser.

15. Installez le certificat dans votre browser en cliquant sur le bouton Click here to install your certificate.

16. Si vous recevez une fenêtre similaire à celle ci-dessous, cliquez sur Yes

Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

17. Vous recevrez ensuite un message indiquant que le certificat a été correctement installé dans votre browser. Cliquez sur le bouton OK.

18. Cliquez sur le bouton **Logout** pour quitter l'application.

19. Vous recevez un écran de confirmation. Cliquez sur Continue pour terminer votre session sécurisée avec la BNB.

5. PROCÉDURE DE RENOUVELLEMENT D'UN CERTIFICAT BNB (RENEWAL)

Notes:

- Il s'agit de la procédure à suivre lorsque vous devez renouveler votre certificat. De fait, les certificats ont une durée de validité limitée à 5 ans; vous serez avertis entre 1 et 3 mois avant l'échéance par l'Autorité d'Enregistrement de la BNB.
- Pour exécuter cette procédure, vous devez être en possession du **Username** (reçu de la BNB) et du **Password** que vous avez choisi. De plus, vous devrez aussi posséder votre **Activation Code** qui vous a été attribué par la BNB.
- Au terme de cette procédure, vous disposerez d'un nouveau certificat. L'ancien certificat reste cependant utilisable jusqu'à son échéance.

1. Dans le Browser Internet, spécifiez l'URL (parfois aussi appelée adresse Internet):
   https://ssl.nbb.be/nbbxenroll

2. Vous recevez un écran invitant à introduire un **Username** et **Password**.

3. Introduisez votre **Username** et le **Password** que vous avez choisi et cliquez sur Log In

4. Cliquez sur **Certificate Renewal**

5. Vous devez marquer votre accord sur les dernières versions des « Certificate Policy » et « Certificate Practice Statement ». Ces dernières versions sont consultables via les liens repris à gauche de la page.

6. Pour marquer votre accord sur ces documents, vous devez cochez la case **I have read and accept the latest Certificate Policy and Certificate Practice Statement documents**. C'est seulement après cette action que le bouton Request certificate deviendra actif.

7. Le champ Email contient l'adresse e-mail qui sera reprise dans le certificat. Cette information peut être utilisée par la banque pour vous contacter. Si l'adresse indiquée n'est plus correcte, veuillez la modifier.

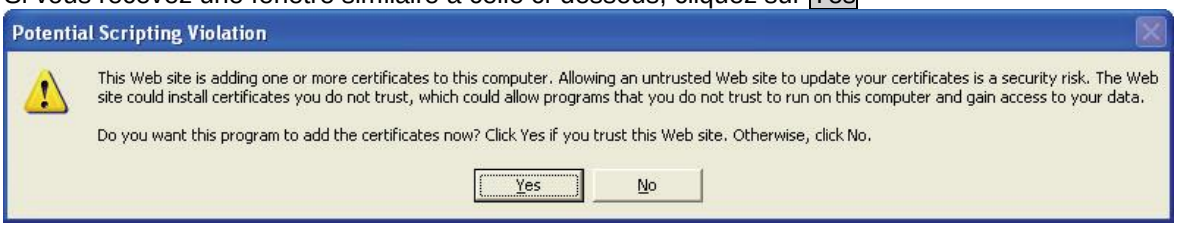
8. Complétez le champ **Activation code** avec le code que vous avez reçu de la Banque.

9. Cliquez sur le bouton Request certificate.

10. Votre PC va générer une clé cryptographique et demander à l'AC BNB de créer le certificat associé. Après quelques instants, vous allez recevoir un écran vous invitant à charger ce certificat dans votre browser.

11. Installer le certificat dans votre browser en cliquant sur le bouton Click here to install your certificate.

12. Si vous recevez une fenêtre similaire à celle ci-dessous, cliquez sur Yes


Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

13. Vous recevrez ensuite un message indiquant que le certificat a été correctement installé dans votre browser. Cliquez sur le bouton OK.

14. Cliquez sur le bouton **Logout** pour quitter l'application.

15. Vous recevez un écran de confirmation. Cliquez sur Continue pour terminer votre session sécurisée avec la BNB.

6. PROCÉDURE DE RÉGÉNÉRATION D'UN CERTIFICAT BNB (RECOVERY)

Notes:

- Cette procédure est essentiellement d'application dans les deux cas suivants:
  1. si le certificat et la clé cryptographique associée sont devenus inutilisables (par exemple en cas de crash machine, de disque dur défectueux, d'un autre problème logique ou physique avec votre PC, ...).
  2. si vous suspectez que le certificat et sa clé cryptographique puissent être utilisés indûment (par exemple si un utilisateur qui a eu accès au certificat et à la clé cryptographique change de fonction ou quitte l'entreprise, ...).
- Pour exécuter cette procédure, vous devez être en possession du **Username** (reçu de la BNB) et du **Password** que vous avez choisi. De plus, vous devrez aussi posséder votre **Activation Code** qui vous a été attribué par la BNB.
- Au terme de cette procédure, vous disposez d'un nouveau certificat. L'ancien certificat est révoqué et ne sera donc probablement plus utilisable dans les applications BNB.

1. Dans le Browser Internet, spécifiez l'URL (parfois aussi appelée adresse Internet):
   https://ssl.nbb.be/nbbxenroll

2. Vous recevez un écran invitant à introduire un **Username** et **Password**.

3. Introduisez les **Username** et le **Password** (que vous avez choisi) et cliquez sur Log In

4. Cliquez sur **Certificate Recovery**

5. Vous devez marquer votre accord sur les dernières versions des « Certificate Policy » et « Certificate Practice Statement ». Les dernières versions de ces documents sont consultables via les liens repris à gauche de la page.

6. Pour marquer votre accord sur ces documents, vous devez cochez la case **I have read and accept the latest Certificate Policy and Certificate Practice Statement documents**. C'est seulement après cette action que le bouton Request certificate deviendra actif.

7. Le champ Email contient l'adresse e-mail qui sera reprise dans le certificat. Cette information peut être utilisée par la banque pour vous contacter. Si l'adresse indiquée n'est plus correcte, veuillez la modifier.

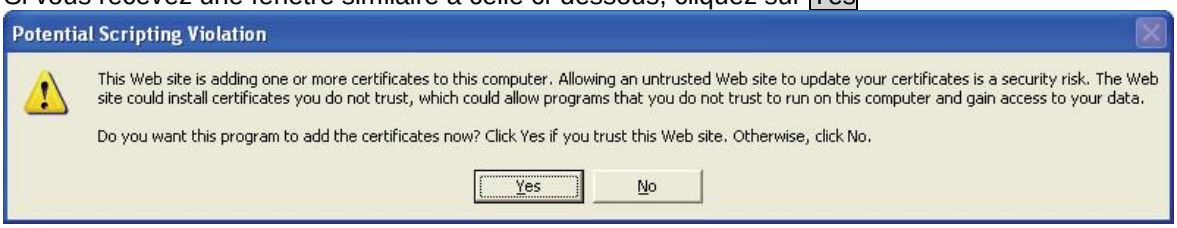
8. Complétez le champ **Activation code** avec le code que vous avez reçu de la Banque.

9. Cliquez sur le bouton Request certificate.

10. Votre PC va générer une clé cryptographique et demander à l'AC BNB de créer le certificat associé. Après quelques instants, vous allez recevoir un écran vous invitant à charger ce certificat dans votre browser.

11. Installer le certificat dans votre browser en cliquant sur le bouton Click here to install your certificate.

12. Si vous recevez une fenêtre similaire à celle ci-dessous, cliquez sur Yes


Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

13. Vous recevrez ensuite un message indiquant que le certificat a été correctement installé dans votre browser. Cliquez sur le bouton OK.

14. Cliquez sur le bouton **Logout** pour quitter l'application.

15. Vous recevez un écran de confirmation. Cliquez sur Continue pour terminer votre session sécurisée avec la BNB.

7. PROCÉDURE D'EXPORT, DE SAUVEGARDE/RESTAURATION ET DE SUPPRESSION DE CLÉS ET CERTIFICATS BNB

Pour décharger la dernière version de ces procédures, procédez comme suit :

1. Dans le Browser Internet, spécifiez l'URL (parfois aussi appelée adresse Internet):
   https://ssl.nbb.be/nbbxenroll

2. Vous recevez un écran invitant à introduire un **Username** et **Password**.

3. Introduisez les **Username** et le **Password** (que vous avez choisi) et cliquez sur Log In

4. Cliquez sur **Downloads**

5. Effectuez un click-droit sur **Certificate management documentation** pour décharger le manuel dans la langue de votre choix

6. Sélectionner Save Target As... et indiquer l'emplacement où vous voulez sauvegarder le fichier (par exemple « D:\Temp »)

7. Cliquez sur le bouton **Logout** pour quitter l'application.

8. Vous recevez un écran de confirmation. Cliquez sur Continue pour terminer votre session sécurisée avec la BNB.

9. Ouvrez le manuel que vous venez de sauvegarder et suivez les instructions.

8. PROCÉDURE DE DÉCHARGEMENT DU PROGRAMME FACULTATIF « OFFLINE SIGNING TOOLS » (OST)

1. Dans le Browser Internet, spécifiez l'URL (parfois aussi appelée adresse Internet):
   https://ssl.nbb.be/nbbxenroll

2. Vous recevez un écran invitant à introduire un **Username** et **Password**.

3. Introduisez les **Username** et le **Password** (que vous avez choisi) et cliquez sur Log In

4. Cliquez sur **Downloads**

5. Cliquez sur **Offline signing tool** pour décharger le programme

6. Dans la fenêtre de « download », cliquez Save

7. Dans la sauvegarde, choisissez l'emplacement où vous voulez sauvegarder le fichier (par exemple « D:\Temp ») puis cliquez sur Save

8. Effectuez un click-droit sur **OST User guide** pour décharger le manuel d'utilisation

9. Sélectionner Save Target As... et indiquer l'emplacement où vous voulez sauvegarder le fichier (par exemple « D:\Temp »)

10. Cliquez sur le bouton **Logout** pour quitter l'application.

11. Vous recevez un écran de confirmation. Cliquez sur Continue pour terminer votre session sécurisée avec la BNB.

12. Ouvrez le manuel que vous venez de sauvegarder et suivez les instructions.

9. PROCÉDURES SPÉCIALES

Si vous avez OUBLIÉ le **Password** que vous avez choisi au cours de la « Procédure de génération d'un certificat », vous devez informer votre point de contact BNB qui remettra ce **Password** à la valeur initiale telle qu'indiquée sur le document reçu de la BNB.

Si vous avez OUBLIÉ le **Password** initial ou **l'Activation code** reçus de la BNB, vous devez informer votre contact à la BNB et vous présenter personnellement auprès de l'Autorité d'Enregistrement de la BNB pour recevoir de nouveaux codes.